provided by a protective cover disposed thereon, the chemical eraser unit **450** may be the preferred choice.

In yet another aspect of the invention, a guard system may further be arranged to degrade information stored in volatile memory devices such as a RAM and/or other non-volatile memory devices such as a flash memory. For example, the guard system **400** may be electrically connected to those memory devices such that the guard system **400** may disconnect power supply thereto and/or supply sufficiently high current which may alter or disrupt capacitive properties of such devices.

In yet another aspect of the invention, an optical and/or laser disks may also be protected by a guard system. The guard system may be provided with at least one laser gun capable of emitting laser beams. Upon receiving a protection command signal from the signal generating unit **330** of the access control system **300**, the guard system fires laser beams onto the tracks formed on the surfaces of such disks. The intensity of the laser beams may be adjusted such that the beams leave dark marks on the tracks, thereby degrading the information retrieved by an optical and/or laser disk drive.

It is to be understood that while the present invention has been described in conjunction with the detailed description thereof, the foregoing description is intended to illustrate and not limit the scope of the invention, which is defined by the scope of the appended claims. Other aspects, advantages, and modifications are within the scope of the following claims.

What is claimed is:

1. A computer capable of protecting information stored in a hard disk thereof from being accessed by an unauthorized user comprising:

an access control system capable of detecting unauthorized attempt to access said information and generating a protection command signal responsive to said attempt; and

a guard system capable of degrading at least a portion of said information responsive to said protection command signal.

2. A computer capable of protecting information processed thereby from being accessed by an unauthorized user comprising:

at least one information processing system for processing said information;

an access control system capable of detecting unauthorized attempt to access said information and generating a protection command signal responsive to said attempt; and

a guard system capable of degrading at least a portion of said information responsive to said protection command signal.

3. The computer according to claim 2, wherein said information processing system comprising at least one information storage unit and further comprising at least one of:

an information read-only unit;

an information write-only unit; and

an information read/write unit.

4. The computer according to claim 3 wherein information is stored in said information storage unit as a plurality of magnetic bands formed on a surface of said information storage unit.

5. The computer according to claim 3 wherein information stored in said information storage unit comprises at least one of:

a digitized program;

a digitized datum;

a digitized sound; and

a digitized image.

6. The computer according to claim 3 wherein said information storage unit and said information read/write unit comprise, respectively, at least one of:

a hard disk and a hard disk driver;

a floppy disk and a floppy disk driver; and

a magnetic tape and a magnetic tape driver.

7. The computer according to claim 3 wherein said access control system further comprises:

an input receiving unit for receiving a log-in input; and

a logic unit for determining validity of said log-in input, said logic unit providing access to said computer when said log-in input is valid but sending said protection command signal to said guard system when said log-in input is invalid.

8. The computer according to claim 3 wherein said guard system further comprises:

a signal receiving unit for receiving a command signal from said access control system wherein said command signal comprises said protection command signal; and

an eraser unit for degrading at least a portion of information stored in said information storage unit.

9. The computer according to claim 8 wherein said eraser unit is disposed adjacent said information storage unit and comprises at least one chamber having therein at least one chemical substance capable of altering magnetic property of said information storage unit, said eraser unit configured to deliver said chemical substance from said chamber to said information storage unit responsive to said protection command signal.

10. The computer according to claim 8 wherein said eraser unit is disposed adjacent said information storage unit and comprises at least one chamber having therein at least one chemical substance capable of forming a substantially non-peelable bonding with

said information storage unit, said eraser unit configured to deliver said chemical substance from said chamber to said information storage unit responsive to said protection command signal.

11. The computer according to claim 8 wherein said eraser unit is disposed adjacent said information storage unit and comprises at least one mechanical member capable of mechanically deforming said information storage unit upon contact therewith.

12. The computer according to claim 8 wherein said eraser unit is disposed adjacent said information storage unit and capable of generating magnetic field around at least a portion of said information storage unit responsive to said protection command signal.

13. The computer according to claim 8 wherein said guard system further comprises a motion device capable of moving at least one of said eraser unit and said information storage unit with respect to the other of said erasure unit and said information storage unit.

14. The computer according to claim C15 wherein said eraser unit further comprises a motion device capable of moving said eraser unit while said eraser unit generates magnetic field therearound.

15. A method of protecting information processed by a computer from being accessed by an unauthorized user comprising the steps of:

detecting unauthorized attempt to access said information; and

degrading at least a portion of said information upon detecting said unauthorized attempt.

16. The method according to claim 15 wherein the detecting step comprises the steps of:

receiving a log-in input; and

determining validity of said log-in input.

17. The method according to claim 15 wherein the detecting step comprises the steps of:

sensing a disassembly capable of exposing an interior of said computer; and

determining validity of said disassembly.

18. The method according to claim 15 wherein said degrading step comprises the steps of:

contacting at least a portion of said computer with at least one chemical substance, said portion storing said information; and

altering chemical property of said portion of said computer.

19. The method according to claim 15 wherein said degrading step comprises the steps of:

contacting at least a portion of said computer with at least one chemical substance, said portion storing said information; and

altering mechanical property of said portion of said computer.

20. The method according to claim 15 wherein said degrading step comprises the steps of:

contacting at least a portion of said computer with at least one chemical substance, said portion storing said information; and

altering magnetic property of said portion of said computer.